RCA PF030097AA

CITED BY APPLICANT

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 November 2000 (30.11.2000)

PCT

(10) International Publication Number
WO 00/72504 A1

(51) International Patent Classification[7]: H04L 9/30, 9/08

(21) International Application Number: PCT/GB00/01950

(22) International Filing Date: 25 May 2000 (25.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9911986.9 25 May 1999 (25.05.1999) GB
9913601.2 12 June 1999 (12.06.1999) GB

(71) Applicant *(for all designated States except US)*: nCIPHER CORPORATION LIMITED [GB/GB]; Jupiter House, Station Road, Cambridge CB1 2JD (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: HARVEY, Ian [GB/GB]; nCipher Corporation Limited, Jupiter House, Station Road, Cambridge CB1 2JD (GB). VAN SOMEREN, Nicko [GB/GB]; nCipher Corporation Limited, Jupiter House, Station Road, Cambridge CB1 2JD (GB).

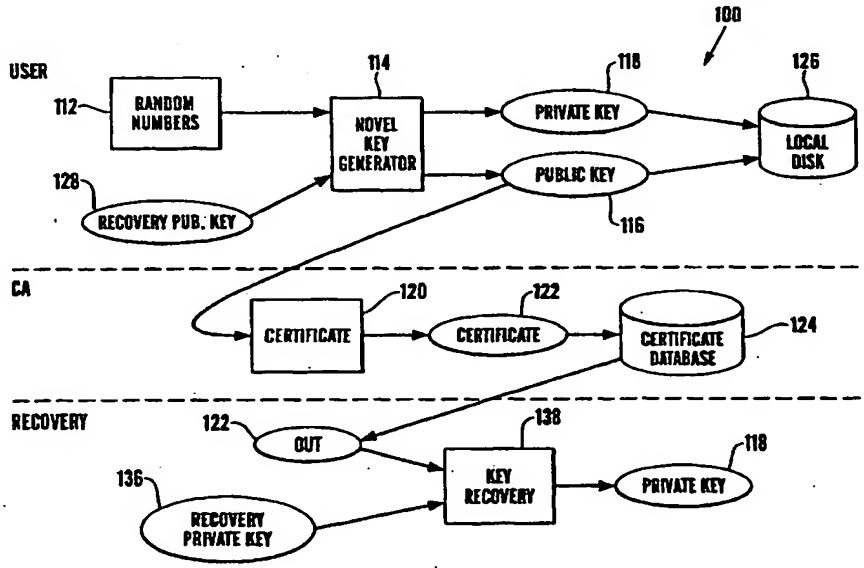
(74) Agent: HALLAM, Arnold, Vincent; 144 New Walk, Leicester LE1 7JA (GB).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PRIVATE KEY RECOVERY



(57) Abstract: A method of cryptographic key generation comprises generating a public key and a private key wherein the public key contains all of the information required to recover the private key. The private key can be recovered from the public key by an authorised third party with access to a private recovery key. The need for the private key to be separately archived is therefore eliminated.

WO 00/72504 A1

Published:

— *With international search report.*

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PRIVATE KEY RECOVERY

The present invention relates to key recovery and particularly, but not exclusively, to a method for the recovery of cryptographic keys in secure computer systems.

In business applications, one of the biggest risks when using cryptographic computer systems is that if a legitimate user loses their private "key" then they may be unable to gain access to the cryptographic system. The loss of the key may be as a result of the user forgetting a password or because a member of staff within an organisation has left the organisation taking the key with them.

In order to address this problem many cryptographic systems employ a facility know as "key recovery". This is a process whereby the user can store their key in safe place such that if at some later stage the key is lost it may be recovered by a third party (such as an officer of the organisation). Existing key recovery methods are generally complex involving a large number of steps both on the part of the user and the recovery officer and necessitates the maintenance of an excessive number of storage facilities such as databases.

The present invention aims to provide an improved method for recovering cryptographic keys.

Accordingly, the present invention provides a method of cryptographic key generation comprising generating a private key and a public key, wherein said public key contains information about said private key therein.

Preferably, the public key contains all of the information required for recovery or regeneration of the private key.

The present invention will now be described, by way of example only, with reference to the

accompanying drawings in which;

Figure 1 is a schematic block diagram of a typical key cryptographic computer system including key generation and recovery architecture according to the prior art;

Figure 2 is a block diagram illustrating a method of generating a cryptographic key in the system of figure 1;

Figure 3 is a schematic block diagram of a preferred form of computer system incorporating key generation and recovery architecture according to the invention;

Figure 4 illustrates a preferred method of key generation according to the invention;

Figure 5 illustrates a preferred method of key recovery according to the invention;

Figure 6 illustrates a relationship between the methods of figures 4 and 5; and

Figure 7 is a table of preferred algorithms for use in the methods shown in figures 4 to 6.

In public key cryptographic systems (also know as asymmetric cryptographic systems) a user generates a pair of cryptographic keys, one of which is made available to all other users (known as the public key) and the other of which is kept secret (known as the private key). The public key is used for public functions such as encrypting a message to send to the user or for verifying a digital signature which was supposedly made by that user. The private key, on the other hand is used for private functions such as decrypting a received message or applying a digital signature. The public key will usually be authorised by a body known as a Certification Authority (CA) which stores the public key in a database and distributes it to any other person who may want it. The private key will usually be kept in a safe place and will only be known to the user.

If the user's private key is lost for any reason, the user may be unable to access many applications of the cryptographic system. Consequently, most cryptographic systems feature key recovery mechanisms for recovering lost keys and avoiding data loss. Existing key recovery mechanisms conventionally require a pro-active approach in which extra data must be generated and stored by the user over and above that which is made public.

Referring to Figure 1, a typical cryptographic system architecture involving key generation and recovery facilities is shown in schematic block form generally at 10. In the key generation stage a random number generator 12 generates a number which is supplied to a main key generator block 14 which applies one or more predetermined algorithms to the random number in order to generate a public key 16 and a private key 18. The public key 16 is passed to a certification generator 20 which generates a digital certificate 22 of the key and the certificate is then stored in a public database 24.

The user stores a copy of the private key 18 in a local storage device such as hard disc 26. In addition, the private key 18 and a further public key 28 which is held by a third party responsible for key recovery (hereafter "key recovery agent") are applied to an encryption system 30 which generates an encrypted "key archival object" 32 which is then stored in a private key recovery database 34.

If, at a later date, the user needs to recover his private key, the key recovery agent extracts the key archival object 32 from the private key recovery database 34 and applies it, together with the recovery agent's private key 36 to a decryption system 38. The decryption system 38 uses the key archival object 32 and the recovery agent's private key 36 to recover the private key 18.

Figure 2 illustrates a standard key generation process for the system of Figure 1. The random number generator 12 feeds into two prime number finders 40, 41 each of which is also supplied with a public exponent E. The outputs P, Q of the prime number finders 40, 41 are applied, together with the public exponent E, into a private key generator 42, forming part

of the main key generator block 14. The private key generator 42 generates an output D.

The outputs P, Q of the prime number finders 40, 41 are also fed into a public key generator 44 which generates an output N. The outputs P, Q and D therefore represent the private key 18 and the components E and N represent the public key 16.

The above described system achieves the requirement for key recovery but has a number of disadvantages. For example, the method involves a large number of steps both on the part of the user and the key recovery agent and also requires the maintenance of two databases, one for the digital certificates and one for the key recovery objects. In addition, the user is required explicitly to add their private key to the key recovery database 34.

Referring to Figure 3, a preferred form of cryptographic system having key generation and recovery facilities is shown generally at 100. The invention allows the secure key archival to be coupled closely with the key generation and certification process.

In Figure 3, a random number generator 112 generates a random number which is applied, together with the public key of the recovery agent 128 to a main key generator 114. The main key generator generates a public key 116 and a private key 118. As previously, the public key 116 is passed to a certification generator 120 which makes a digital certificate 122 of the public key 116 which is then stored in a public database 124. In addition, the user stores a copy of the private key 118 on a local storage device or hard disc 126. No further action is required on the part of the user since all of the information necessary for key recovery is embedded in the public key 116.

At a later date, if the user needs to recover the private key, a copy of the public key 116 is extracted from the digital certificate 122 stored in the database 124. The copy is passed to a key recovery system 138 together with the recovery agent's private key 136. The key recovery system 138 produces a recovered private key which should be identical to the original private key 118.

It should be noted that if the key generation process is trusted, then the recovery agent's public and private keys can be identical and a symmetrical version of the key generation process and key recovery process can be used.

Referring to Figure 4, a key generation mechanism according to the invention is shown in schematic form. In this mechanism, the random number generator 112 generates two random values A and B. The value A is sent to a functional unit designated H along with the recovery agent's public key 128. The output of the unit H is a value U. The value A and the recovery agent's public key 128 are also applied to a second functional unit G which generates a value C. The values B and C are combined in a joiner unit 148 in such a way that the data of the value C represents the output N′ of the joiner unit 148 while the data of value B represent the less significant bit of N′. The values U, N′ are then applied to a factorisation unit 150 together with the public exponent E in the following manner:

N′ and U are assumed to represent respectively the product and the sum of data P′ and Q′ and the values of these are computed using basic mathematical relationships. The factorisation unit 150 then searches for the value P which is the smallest prime number greater than or equal to P′ which is suitable for use in a cryptographic key. The factorisation unit 150 then searches for a value Q which is the largest prime number less than or equal to Q′ which is also suitable for use in a key.

Once the factorisation unit 150 has output the values P and Q, they are processed by a public key generator 144, which forms part of the main key generator block 114, to produce the public value N. The values P and Q are also applied with the public exponent E to the private key generator 142, also forming part of the main key generator block 114, to generate the value D. These processes are similar to those of Figure 2.

A check is then made that the more significant bits of N are the same as the more significant bits of N′. If this is not the case, then the process is restarted. The final public key is represented by the components E and N while the private key 118 is represented by the

components P, Q and D as in the case of Figure 2.

Referring to Figure 5, a key recovery process according to the invention is shown in schematic form. In this process, the value N is taken from the public key 116 and split by a splitter unit 152 into two parts, a part containing the more significant bits and a part containing the less significant bits. It should be noted that this is the reverse process of the joiner unit 148 illustrated in Figure 4. The less significant bits are discarded. The more significant bits, designated M, are fed into a third functional unit F along with the recovery agent's private key 136 to produce a value U. The values U and N are passed to another factorisation unit 150a which produces values P and Q. The values P and Q are applied, together with the value E extracted from the public key 116, into the private key generation unit 142 to produce the value D. This is similar to the process involved in key generation. The components P, Q and D represent the recovered private key.

Referring to Figure 6, the relationship between the functional units F, G and H is shown in schematic form. The three functional units satisfy the following criteria. Functional units H and G are applied with an input and the public key of the recovery agent 128. Functional unit F is presented with the recovery agent's private key 136 and the output of unit G. Unit F must produce the same output value as unit H when both units G and H have the same input. The functional units F, G and H in the key generation and recovery processes can take a number of forms. These forms are shown in the table of Figure 7. Many variants could be used here, for example, the function sets for RSA or DH could be replaced with versions of these algorithms based on elliptic curve encryption. Furthermore, various different HMAC or symmetric encryption mechanisms could be used in place of the ones shown in Figure 7.

In a preferred form of the invention, the following algorithm is used to generate or recover a key. The key generation algorithm provides built in key recovery and knowledge of the details of the key generation process together with a generated public key is not sufficient to derive the private key. This is very important for preventing unauthorised parties from establishing the private key and gaining access to the system.

Prior to generating the key, three functions are selected. The function F(x, Ks) makes use of the key recovery agent's private key while the functions G(x, Kp) and H(x, Kp) make use of the agent's public key. The three functions together satisfy the relationship:

$$F(G(x, Kp), Ks)=H(x, Kp)$$

and the function G( ) must be a "one-way" function i.e. given the output of the function, it is difficult or impossible to compute the input, but given the input it is easy to compute the output.

The steps for generating a key are as follows:

1. Select a random value x and compute G(x, Kp) and H(x, Kp);

2. Concatenate a one bit, G(x, Kp) and a random value s to generate N′ such that: *msbits*(N′) = G(x, Kp), where *msbits*(N′) is a function which takes a number and returns the most significant 3m/8 of the bits in the binary representation of that number excluding the most significant and where m is the number of bits in the key;

3. Let U = #(H(x, Kp)) where #( ) is a hash function;

4. Check that $2N' < U < (2N'/r) + (r/2)$ where $r = 2^{(m/2)}$ and if not, return to step two;

5. Assume that U = (P+Q) so compute that $V = (P-Q) = (u^2 - 4N')^{1/2}$;

6. Starting at P = (U + V)/2 to search upwards until P is prime;

7. Starting at Q = (U - V)/2, search downwards until Q is prime;

8. Ensure that *msbits*(PQ) = *msbits*(N′); if not start again;

9. Use P and Q to generate the private key using the standard method.

For recovery of the key, the method involves the following steps;

1. Let U = #(F(*msbits*(N), Ks));

2. Assume that U = (P + Q), therefore compute $V = (P - Q)(U^2 - 4N')^{1/2}$;

3. Starting at P = (U + V)/2 search upwards P is prime;

4. Calculate Q = N/P and generate the private key in the standard manner.

Referring to Figure 7, this is a table illustrating some possible functions for use with the above algorithm. This algorithm allows for the secure generation of public and private keys with the property that, by the use of some additional information independent of the key, the private key can be recovered from the public key. The algorithm does not require the key generator to have any knowledge of the recovery parameter but instead uses a public key system to separate the generation and the recovery parameters.

This could be used for a variety of key recovery applications. In most systems, the public key will be more widely known than the private key and therefore much less likely to be lost. The implicit nature of this key recovery system removes the need for action by the user to explicitly store their private key, for example, in a separate database.

It can be seen that the present invention provides a method of recovering a cryptographic key which is greatly simplified compared to existing methods and a cryptographic computer system employing such a method. Several steps are removed from the previous method and the user is no longer required to archive their private key. The invention also removes the need for a separate key recovery database. The new key generation process is designed such

that the keys produced are functionally identical to the output of the standard key generation process. Thus, the method of the present invention can be incorporated into existing applications which make use of public key cryptography with little or no change to the application.

CLAIMS

1. A method of cryptographic key generation comprising generating a private key and a public key, wherein said public key contains information about said private key therein.

2. A method of cryptographic key generation according to Claim 1 wherein said public key contains all of the information required for recovery or regeneration of said private key.

3. A method of cryptographic key generation according to claim 1 or 2 comprising:

generating at least one random number;

applying a first algorithm to said random number together with a first predetermined key thereby to generate said public and private keys; and

storing said public key.

4. A method of cryptographic key generation as claimed in claim 3 further comprising:

retrieving said public key; and

applying a second algorithm to said public key together with a second predetermined key, thereby to recover or regenerate said private key.

5. A method of cryptographic key generation according to claim 3 or claim 4 wherein said first and second predetermined keys are known only to an authorised third party.

6. A method of cryptographic key generation according to claims 3, 4 or 5 wherein said first and second algorithms are symmetrical.

7. A system for generating cryptographic keys comprising:

means for generating a private key and a public key in which there is contained information about said private key;

means for storing said public key; and

means for recovering said private key using said information contained in said public key.

8. A system for generating cryptographic keys according to claim 7 wherein said generating means comprises means for generating first and second random numbers;

a first function unit for applying a first predetermined function to said first random number and a first predetermined key thereby to generate a first output value representative of the sum of a first and a second data value;

a second functional unit for applying a second predetermined function to said first random number and said first predetermined key thereby to generate a second output value;

means for combining said second output value and said second random number thereby to generate a third output value representative of the product of said data values;

means for calculating said first and second data values and generating fourth and fifth output values in dependence thereon;

means for processing said fourth and fifth output values together with a predetermined exponent thereby to generate said private key; and

means for processing said fourth and fifth output values only thereby to generate said public key.

9. A system for generating cryptographic keys according to claim 7 or claim 8 wherein said recovering means comprises means for splitting said public key into first and second parts;

a third functional unit for applying a third predetermined function to said first part together with a second predetermined key thereby to generate said first output value;

means for calculating said first and second data values from said first output value and said public key; and

means for processing said first and second variables together with said first predetermined exponents thereby to recover or regenerate said private key.

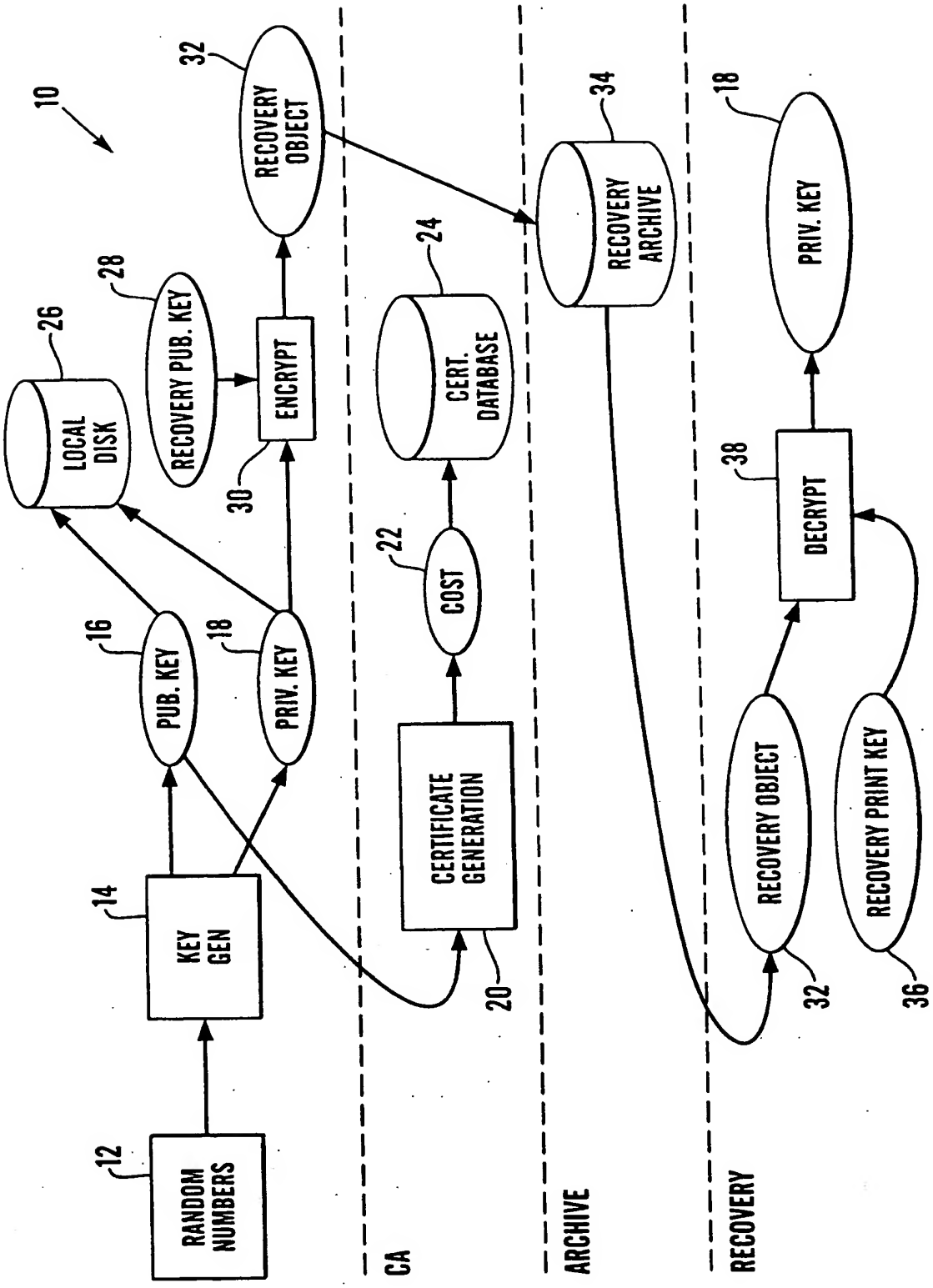

10
RANDOM NUMBERS
12
KEY GEN
14
PUB. KEY
16
PRIV. KEY
18
LOCAL DISK
26
RECOVERY PUB. KEY
28
ENCRYPT
30
RECOVERY OBJECT
32
CERTIFICATE GENERATION
20
COST
22
CERT. DATABASE
24
RECOVERY ARCHIVE
34
PRIV. KEY
18
DECRYPT
38
RECOVERY OBJECT
32
RECOVERY PRINT KEY
36
CA
ARCHIVE
RECOVERY

Fig. 1

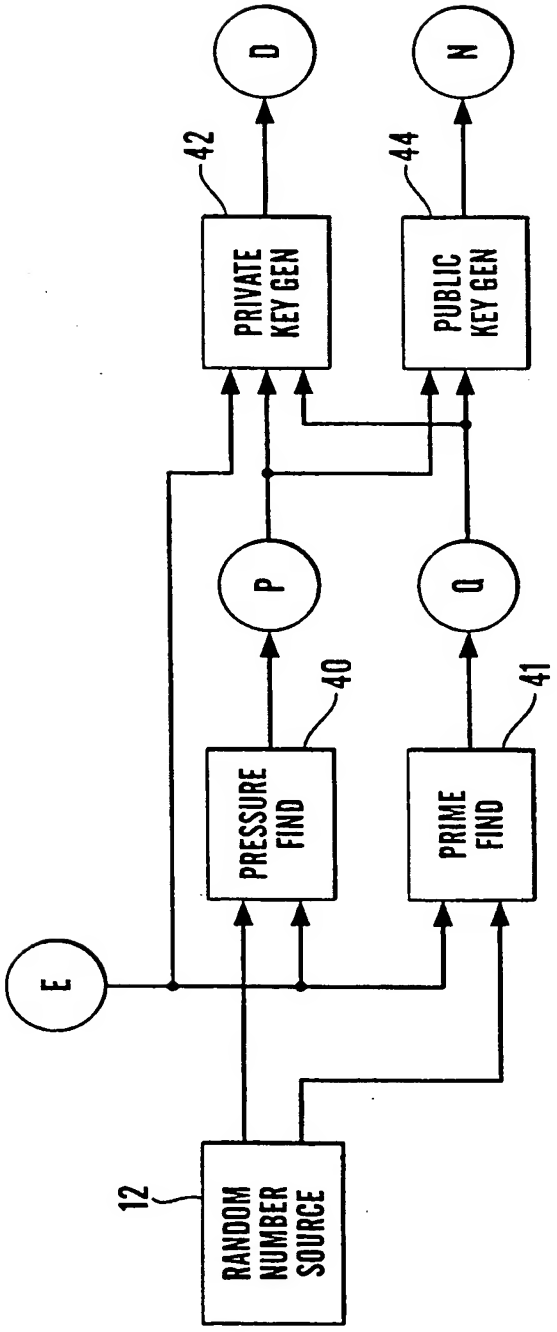

D
N
42
44
PRIVATE KEY GEN
PUBLIC KEY GEN
P
Q
40
41
PRESSURE FIND
PRIME FIND
E
12
RANDOM NUMBER SOURCE

Fig.2

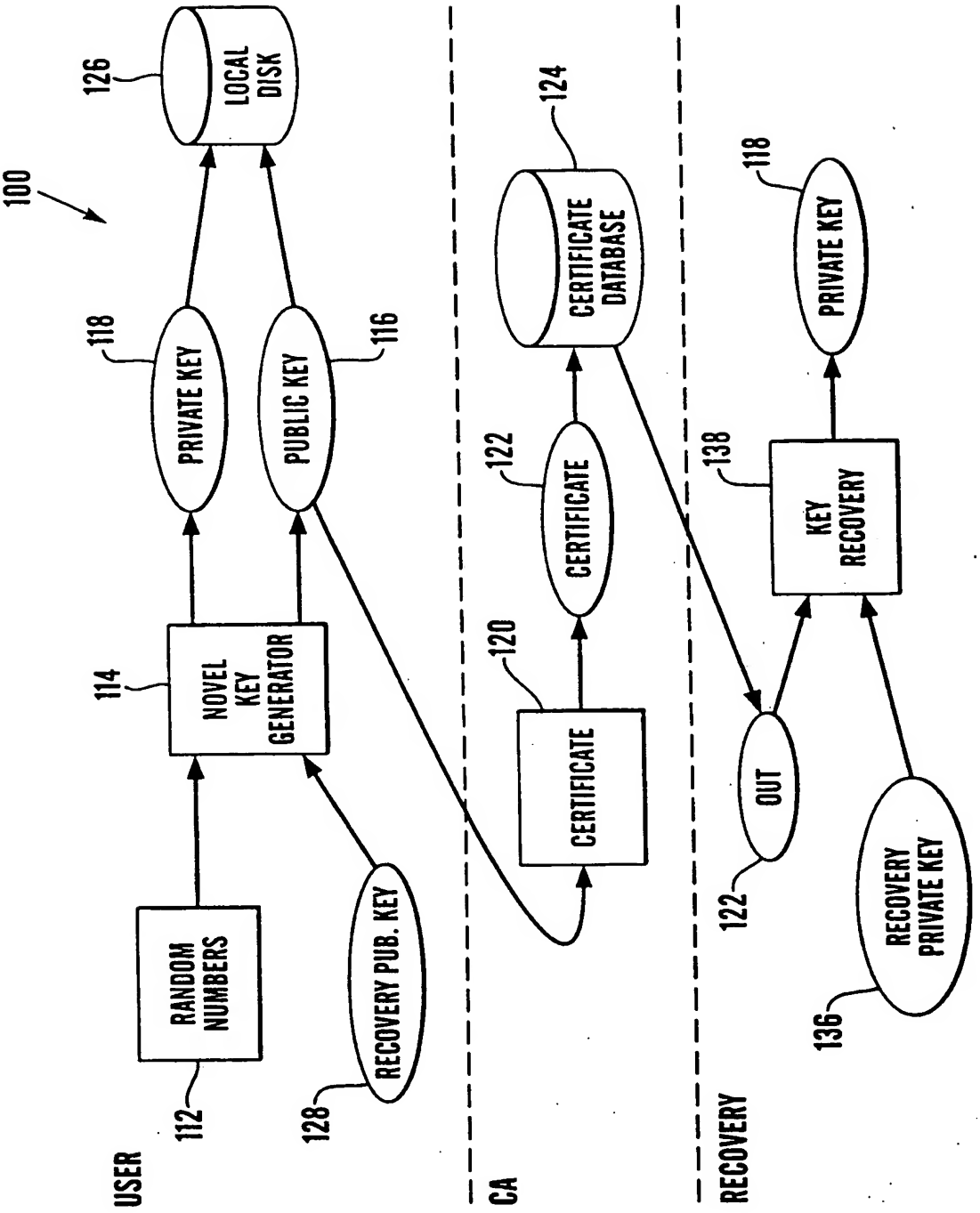

100
126
LOCAL DISK
118
PRIVATE KEY
116
PUBLIC KEY
114
NOVEL KEY GENERATOR
RANDOM NUMBERS
112
RECOVERY PUB. KEY
128
USER
124
CERTIFICATE DATABASE
122
CERTIFICATE
120
CERTIFICATE
CA
118
PRIVATE KEY
138
KEY RECOVERY
OUT
122
RECOVERY PRIVATE KEY
136
RECOVERY

Fig.3

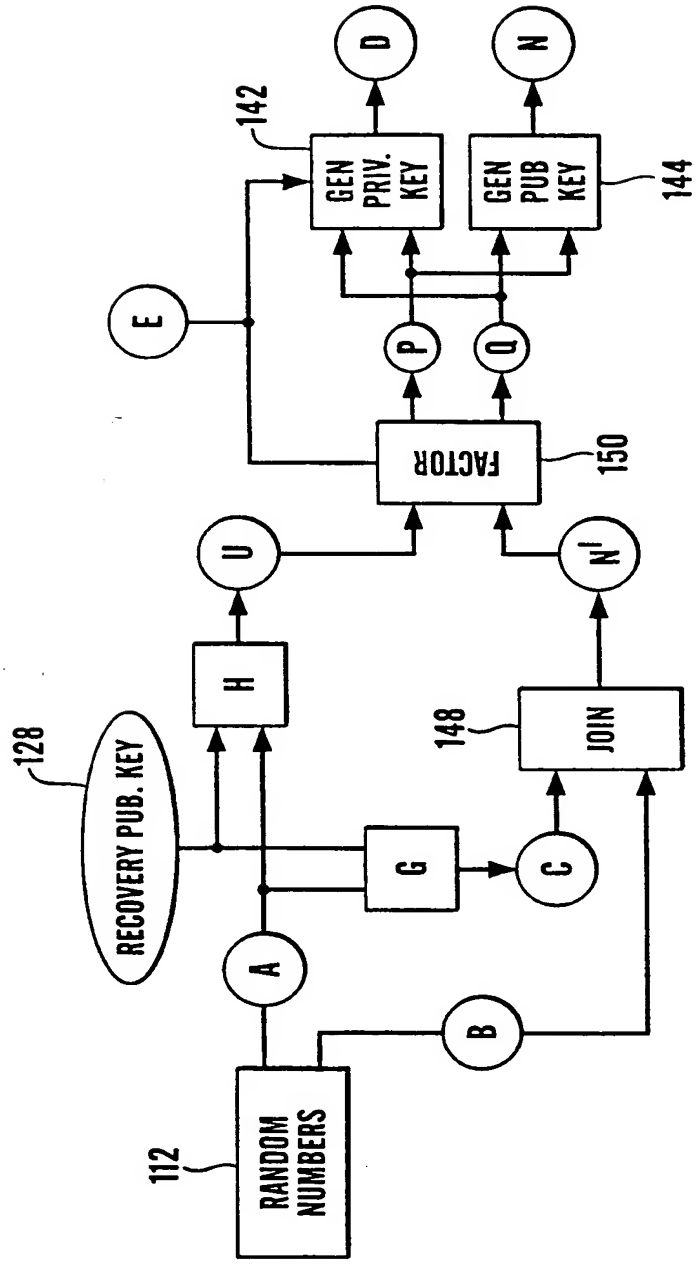

RANDOM NUMBERS
112
RECOVERY PUB. KEY
128
A
B
G
C
H
U
JOIN
148
N'
FACTOR
150
E
P
Q
GEN PRIV. KEY
142
GEN PUB KEY
144
D
N

Fig.4

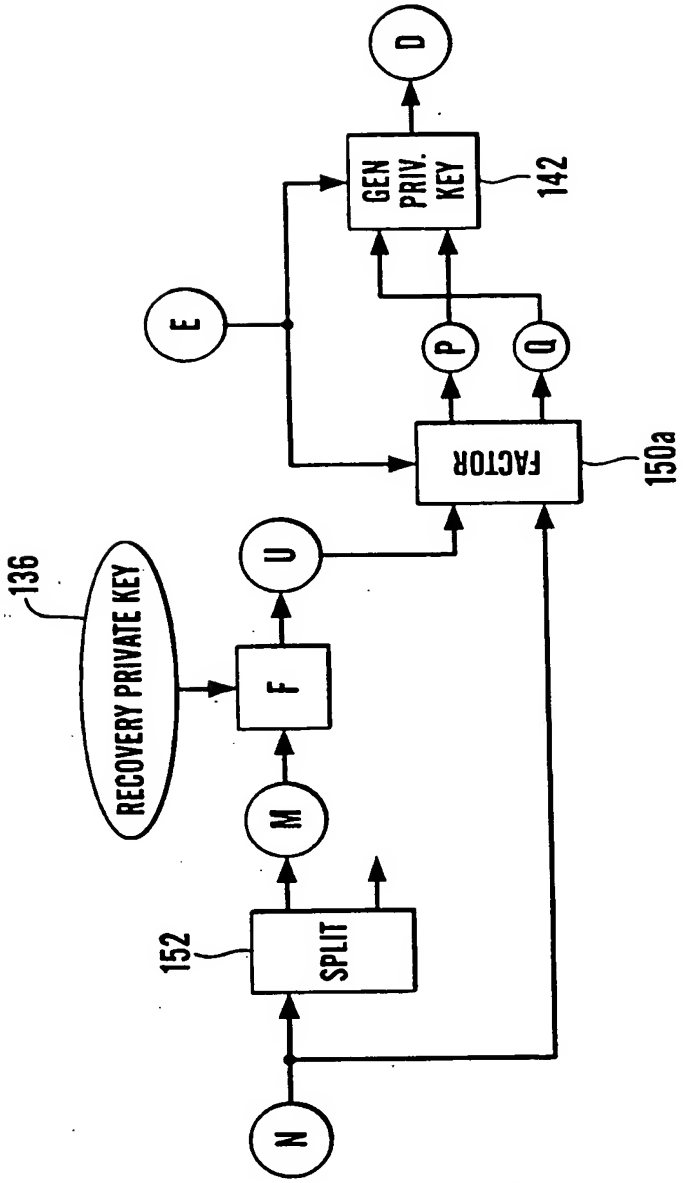

D
GEN PRIV. KEY
142
E
P
Q
FACTOR
150a
U
136
RECOVERY PRIVATE KEY
F
M
152
SPLIT
N

Fig.5

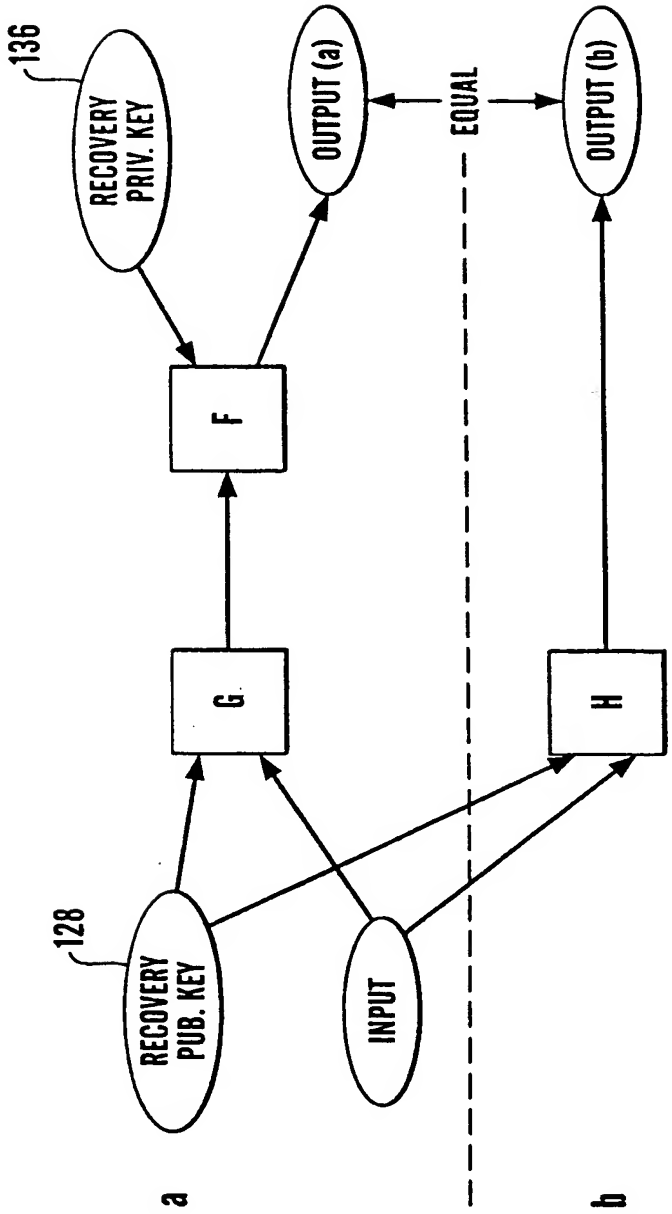

136
RECOVERY PRIV. KEY
OUTPUT (a)
EQUAL
OUTPUT (b)
F
G
H
128
RECOVERY PUB. KEY
INPUT
a
b

Fig.6

Type	F(x,Ks)	G(x,Kp)	H(x,Kp)	Key relation
RSA	$x^{Ks} \bmod n$	$x^{Kp} \bmod n$	x	$Ks.Kp=1 \bmod \phi(n)$
DH	$x^{Ks} \bmod p$	$g^{x} \bmod p$	$(Kp)^{x} \bmod p$	$Kp=g^{Ks} \bmod p$
HMAC	hash(xlKs)	x	hash(xlKp)	Ks=Kp
DES	$DES_{Ks}^{-1}(x)$	$DES_{Kp}(x)$	x	Ks=Kp
EC - DH	Ks.x	x.p	x.Kp	Kp=Ks.p

Fig.7

INTERNATIONAL SEARCH REPORT

Interr nal Application No
PCT/GB 00/01950

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, INSPEC, IBM-TDB, PAJ, COMPENDEX, EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 405 829 A (ADLEMAN LEONARD M ET AL) 20 September 1983 (1983-09-20) column 4, line 14 -column 5, line 17	1,7
A	EP 0 725 512 A (IBM) 7 August 1996 (1996-08-07) abstract column 11, line 17 - line 46	1,7

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 September 2000	18/09/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

ormation on patent family members

Intern nal Application No
PCT/GB 00/01950

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4405829 A	20-09-1983	NONE	
EP 0725512 A	07-08-1996	US 5604801 A	18-02-1997
		JP 8340330 A	24-12-1996